United Nations S/AC.37/2003/(1455)/26

Security Council

Distr.: General
22 April 2003

Original: English

Security Council Committee established pursuant to resolution 1267 (1999)

Letter dated 17 April 2003 from the Permanent Representative of the United States of America to the United Nations addressed to the Chairman of the Committee

The United States Mission hereby submits the report called for under paragraph 6 of resolution 1455 (2003) (see annex). The Government of the United States welcomes the opportunity to describe in detail the steps it has taken to implement the al-Qa`idah/Taliban sanctions regime, which constitutes a key part of the international community's counter-terrorism efforts.

(*Signed*) John D. **Negroponte**

03-35167 (E) 040603

Annex to the letter dated 17 April 2003 from the Permanent Representative of the United States of America to the United Nations addressed to the Chairman of the Committee

Report of the Government of the United States called for under Security Council resolution 1455 (2003)

The United States of America hereby submits the report called for by paragraph 6 of UNSCR 1455 (2003) on all steps taken to implement the measures referred to in paragraph 1 of said resolution. The report follows the guidance prepared by the Committee pursuant to paragraph 12 of the resolution.

I. INTRODUCTION

1. Please provide a description of activities, if any, by Usama bin Laden, Al Qaida, the Taliban and their associates in your country, the threat they pose to the country and the region, as well as likely trends.

Al Qaida and its nexus of associated groups remain the top concern of U.S. law enforcement officials. The United States believes that despite recent setbacks, Al Qaida maintains the ability to inflict significant casualties in the United States with little or no warning.

Moreover, FBI investigations since September 11, 2001 have revealed an extensive and widespread militant Islamic presence in the United States. The activities of the groups we have identified center on fund-raising, recruitment, and training. Their support structure, however, is sufficiently well developed that one or more groups potentially could be activated by Al Qaida to carry out terrorist operations in the United States. There are hundreds of ongoing counter-terrorism investigations in the United States directly associated with Al Qaida.

Subjects of these investigations are primarily located in the East and West coasts and in the Southwest of the United States. We judge the greatest threat to be an Al Qaida cell in the United States that has not yet been detected or identified. Identifying and neutralizing these sleeper cells remains our most serious intelligence and law enforcement challenge. Al Qaida most likely will use the same tactics that were successful on 11 September in carrying out any future attack in the United States, including efforts by cell members to avoid drawing attention to themselves and to minimize contact with militant Islamic groups and mosques in the United States. They will also maintain strict operational and communications security.

The Nature of the Threat

The Al Qaida network will remain for the foreseeable future the most immediate and serious terrorism threat facing the United States. Al Qaida will continue to favor spectacular attacks but also may seek softer targets of opportunity, such as banks, shopping malls, supermarkets, and places of recreation and entertainment.

Al Qaida will continue its efforts to acquire and develop biological, chemical, radiological, and nuclear (CBRN) weapons. We judge that there is a high probability that Al Qaida will attempt an attack using a CBRN weapon within the next two years. The threat of domestic terrorists launching large-scale attacks that inflict mass casualties is low compared to that of international terrorist groups, in part, due to long-standing law enforcement efforts against many of these groups.

Al Qaida does not operate in a vacuum. Many of the groups committed to international jihad offer Al Qaida varying degrees of support. U.S. Government (USG) investigations have revealed a widespread militant Islamic presence in the United States. We strongly suspect that several hundred of these extremists are linked to Al Qaida. However, our investigations have not revealed any evidence that the nexus of organizations and individuals that support Al Qaida's agenda are actively engaged in planning or carrying out a terrorist attack, but

the support structure is sufficiently well-developed that one or more groups or individuals could be used by Al Qaida to carry out operations in the United States or could decide to act independently.

The September 11 terrorists received significant operational funding from overseas, limiting their need to depend on indigenous U.S.-based militant Islamic groups for financial and material support. Subsequent investigations allowed for tracking of the source of those funds and established critical links to other members of the terrorist infrastructure worldwide.

As a result of the media coverage of those events, Al Qaida now knows of our capability to track and monitor such financial activity. Terrorists are therefore more likely to utilize alternative remittance systems and other means of money movement for operational funding to avoid detection by law enforcement and regulatory agencies both before and after planned attacks.

II. CONSOLIDATED LIST

2. How has the 1267 Committee's List been incorporated within your legal system and your administrative structure, including financial supervision, police, immigration control, customs and consular authorities?

Executive Order (E.O.) 13224 provides the legal authority to ensure that the funds and financial or other economic resources of those individuals and entities listed pursuant to UNSCR 1267, 1333, 1390 and 1455 within the United States or within the possession or control of U.S. persons are frozen without delay. This authority is further detailed in the USG report to the 1373 committee (S/2001/1220 pages 6-9, 11). The USG administers sanctions imposed pursuant to E.O. 13224 through the Department of the Treasury's ("Treasury") Office of Foreign Assets Control (OFAC). Additionally, OFAC and the Financial Crimes Enforcement Network (FinCEN) issue and implement regulations to ensure compliance by banks and other financial institutions, as further outlined in question 14.

OFAC provided information on the subject lists of individuals and entities for inclusion in Treasury proprietary information systems accessible to field enforcement personnel with customs, immigration and financial investigations responsibilities. Numerous financial investigations were initiated to identify and freeze assets associated with these individuals and entities.

3. Have you encountered any problems with implementation with regard to the names and identifying information as currently included in the List? If so, please describe these problems.

Due to the list's lack of biographical identifiers and substantive derogatory information indicating inadmissibility to the United States, some of the Taliban-linked individual names have not been entered by immigration authorities into the Legacy INS National Automated Lookout System ("NAILS"). The Lookout System standards require a last name, first name, and year of birth at a minimum and information supporting exclusion or other action. Likewise, in July 2002, this list was shared with the Department of State's "TIPOFF" Lookout Unit and they also concluded that absent derogatory information and biographical identifiers, the TIPOFF unit could not enter the list names in the format presented. Those names that came to Legacy INS and TIPOFF in other formats such as classified cables, which included more identifiers and substantive derogatory information, have been entered into NAILS and TIPOFF.

Some of these names have been entered into TIPOFF and NAILS after being received from other sources along with more identifiers and derogatory information.

As with any such list, the more specific the identifiers, the greater the likelihood that successful enforcement action can take place. Problems associated with the multiple spellings of many names and limitations on identifiers have been widely documented and did cause problems with every agency pursuing investigative leads. The private sector also reports significant difficulties in determining whether name matches are accurate, and has expressed the need for better identifier data.

4. Have your authorities identified inside your territory any designated individuals or entities? If so, please outline the actions that have been taken.

See also answer to Question 6 below.

Operation Green Quest (U.S. Customs, Department of Homeland Security) collects, develops, manages, and disseminates leads to appropriate field offices for appropriate investigative action. As such, it is a repository and clearinghouse for terrorist financial investigations and is able to prioritize and coordinate investigative resources to meet operational goals. Coordination with member agencies and the intelligence community is achieved through Green Quest's systematic vetting process and deconfliction at the field and headquarters level. E.O. 13224 blocks the assets of persons designated pursuant to the E.O., including Al Qaida and the Taliban and persons associated with them. Since September 11, 2001, the United States has frozen $29.9 million in accounts in U.S. jurisdiction of individuals and entities listed on the 1267 Committee consolidated list. Of this amount, $3.1 million is linked to individuals and entities based in the United States that have also been listed on the 1267 Sanctions Committee's consolidated list. (Note: USG policy is generally not to comment specifically on pending investigations or litigation.)

5. Please submit to the Committee, to the extent possible, the names of individuals or entities associated with Usama bin Laden or members of the Taliban or Al Qaida that have not been included in the list, unless to do so would compromise investigations or enforcement actions.

When the Customs and Immigration and Naturalization Services develop leads on possible members or associates of the Al Qaida network or the Taliban, those leads are routinely turned over to the FBI Joint Terrorism Task Force for investigation. The USG cannot comment further on pending investigations or litigation.

6. Have any listed individuals or entities brought a lawsuit or engaged in legal proceedings against your authorities for inclusion in the List? Please specify and elaborate, as appropriate.

No listed individuals or entities have brought legal actions in the United States challenging their inclusion in the UN 1267 Sanctions Committee list. Several listed entities and one individual have, however, filed suit in U.S. courts challenging their designation under the domestic authority of E.O. 13224 and the International Emergency Economic Powers Act (IEEPA). These legal challenges are as follows:

Global Relief Foundation v. Snow, No. 02-CV-674 (N.D. Ill. filed Jan. 28, 2002) (pending).

Benevolence International Foundation v. O'Neill, No. 02-CV-763 (N.D. Ill. filed Jan. 30, 2002) (case dismissed by plaintiff Feb. 25, 2003).

Aaran Money Wire Service, Inc. v. United States, No. 02-CV-789 (D. Minn. filed Apr. 15, 2002) (entities and individual delisted under E.O. 13224, motion to dismiss pending).

Holy Land Foundation v. Ashcroft, No. 02-CV-442 (D.D.C. filed March 8, 2002) appeal pending before the D.C. Court of Appeals.

7. Have you identified any of the listed individuals as nationals or residents of your country? Do your authorities have any relevant information about them not already included on the list? If so, please provide this information to the Committee as well similar information on listed entities, as available.

None of the listed individuals is a U.S. national or resident. One previously listed individual who is a U.S. resident was removed from the list.

8. According to your national legislation, if any, please describe any measures you have taken to prevent entities and individuals from recruiting or supporting Al Qaida members in carrying out activities inside your country, and to prevent individuals from participating in Al Qaida training camps established in your territory or in another country.

The United States relies both on administrative measures and on criminal provisions to prevent and suppress the provision of support to Al Qaida from within the United States or by U.S. persons, wherever located. The goal of the U.S. terrorist support enforcement program is two-fold: (1) to prevent terrorist acts before they occur, by inserting law enforcement at the earliest stages of conspiratorial planning, and (2) to create an environment in which persons are deterred from providing anything of value to any terrorist organization.

Al Qaida has been designated pursuant to two separate Executive Orders, E.O. 13224 and E.O. 12947, as amended by E.O. 13099 of August 20, 1998, and has been designated as a "foreign terrorist organization" (FTO) pursuant to section 219 of the Immigration and Nationality Act, as amended. As a result of its designation under E.O. 13224 in September 2001, its assets in the United States or held by U.S. persons are blocked and all transactions with Al Qaida are generally prohibited. Persons who violate the Executive Order may be subject to both civil and criminal penalties. In addition, because Al Qaida has been designated as an FTO, it is a crime for anyone subject to the jurisdiction of the United States to knowingly provide, to attempt to provide, or to conspire to provide, "material support or resources" to Al Qaida. {Title 18, United States Code (U.S.C.) § 2339B}. The definition of "material support or resources" in 18 U.S.C. § 2339A would cover the training of members of a designated FTO within the United States.

Indeed, the United States has charged several persons for conspiring to engage in or engaging in such conduct, even where the ultimate goal is violence abroad. We have also charged and obtained guilty pleas from several persons within the United States who trained at Al Qaida camps overseas, based on the theory that they sought to provide their own services to that terrorist group. These cases have relied on foreign intelligence and counterintelligence developed by the U.S. intelligence community, which can be more easily shared with U.S. law enforcement as a result of the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT Act). (See below for details on the Act.)

III. FINANCIAL AND ECONOMIC ASSET FREEZE

Under the sanctions regime (paragraph 4(b) of resolution 1267 (1999) and paragraphs 1 and 2(a) of resolution 1390 (2002), States are to freeze without delay the funds and other financial assets or economic resources of the listed individuals and entities, including funds derived from property owned or controlled, directly or indirectly, by them or by persons acting on their behalf or at their direction, and ensure that neither these nor any other funds, assets or resources are made available, directly or indirectly, for such persons' benefit, by their nationals or by any persons within their territory.

NOTE: For the purpose of implementation of the financial prohibitions in this sanctions regime, "economic resources" is defined to mean assets of every kind, whether tangible or intangible, movable or immovable. (Footnote 1: From the International Convention for the Suppression of the Financing of Terrorism, 1999)

9. Please describe briefly:

- **the domestic legal basis to implement the asset freeze required by the resolutions above;**
- **any impediments under your domestic law in this context and steps taken to address them.**

E.O. 13224 provides the domestic legal basis to implement the obligations to freeze the assets of individuals and entities listed pursuant to UNSCRs 1267, 1333, 1390 and 1455. This authority is further detailed in the USG report to the 1373 Counter-Terrorism Committee (S/2001/1220 pages 6-9, 11).

10. Please describe any structures or mechanisms in place within your Government to identify and investigate Usama bin Laden, Al Qaida or Taliban-related financial networks, or those who provide support to them or individuals, groups, undertakings and entities associated with them within your jurisdiction. Please indicate, as appropriate, how your efforts are coordinated nationally, regionally and/or internationally.

There are multiple structures and mechanisms within the USG to identify, investigate and disrupt the financial networks of terrorists including Usama bin Laden, Al Qaida and the Taliban.

The Department of State, Treasury, the Department of Justice, the Department of Homeland Security, intelligence agencies, law enforcement agencies, and the White House (National Security Council -- NSC) work together closely to identify, track and pursue terrorist financing targets and to encourage the international community to take measures and adopt rules and regulations designed to undermine the ability of terrorists to raise and channel funds. The Terrorism Financing Policy Coordination Committee (PCC), established under the directive of the National Security Council and chaired by the Treasury, directs and coordinates the interagency efforts to understand and disrupt terrorism financing networks.

Entities

The following entities and authorities (which are further delineated in UNSC S/2002/674, pages 3-4; UNSC S/2001/1220, pages 4-12) assist in the identification and investigation of terrorist financing networks:

OFAC – Treasury's Office of Foreign Assets Control identifies, investigates, and designates, in consultation with the Departments of Justice, State and Homeland Security, terrorism-related individuals and entities under the authority of E.O. 13224. OFAC maintains and disseminates the list of persons designated under E.O. 13224. OFAC also works with banks, financial institutions, and other U.S. persons to ensure compliance with relevant U.S. laws, executive orders and regulations related to terrorism financing within the scope of its jurisdiction.

Department of State – The Coordinator for Counter-terrorism (S/CT) and the Bureau of Economic and Business Affairs (EB) identify and work with intelligence and international partners to designate, in consultation with the Departments of Justice, Treasury and Homeland Security, terrorists under E.O. 13224, and foreign groups as "foreign terrorist organizations" (FTO) under section 219 of the Immigration and Nationality Act, as amended (See answer to question 9 above). The Department of State's Bureau of International Organization Affairs (IO) is charged with coordinating domestic actions against terrorists and their supporters with those actions taken by the international community pursuant to UNSCRs 1267, 1390, and 1455. State's regional bureaus, other functional bureaus, Office of the Legal Adviser, and U.S. diplomatic missions abroad engage as necessary on designations or issues relevant to their expertise.

FinCEN – Treasury's Financial Crimes Enforcement Network is the financial intelligence unit (FIU) for the USG. FinCEN collects, analyzes, and distributes financial information from the private sector (particularly suspicious activity reports -- SARs) in support of law enforcement investigations, including terrorism financing investigations.

Operation Green Quest – Operation Green Quest is an interagency law enforcement body under U.S. Customs of the Department of Homeland Security created to identify, disrupt, and dismantle the financial infrastructure of terrorist organizations.

Federal Bureau of Investigation (FBI) – The Terrorist Financing Operations Section (TFOS) seeks to identify, investigate, prosecute, disrupt, and dismantle all terrorist-related financial and fundraising activities. TFOS is also engaged in an aggressive international outreach program to share information regarding terrorist financing methods with the financial community and law enforcement, and has built upon long-established relationships with the financial services community in the United States and abroad. TFOS regularly shares and coordinates information with Customs and Treasury.

Authorities

The United States is prosecuting the war on terrorism financing utilizing several different domestic authorities (See also UNSC S/2001/1220, pages 6-11.)

Executive Order (E.O.) 13224 - Pursuant to several domestic authorities, including the International Emergency Economic Powers Act (IEEPA) (50 U.S.C. § 1701 et seq.) and section 5 of the United Nations Participation Act of 1945, as amended, (22 U.S.C. § 287c) (UNPA), E.O. 13224 blocks the assets, and prohibits most transactions with, persons designated in or pursuant to the Order. E.O. 13224 provides the Secretaries of State and the Treasury, in consultation with specified agency heads, the authority to designate terrorism-related individuals and entities under the criteria specified in the Executive Order. Persons who violate E.O. 13224 may be subject to civil or criminal penalties. Criminal penalties may result in up to 10 years in prison, or fines of $500,000 for corporations and $250,000 for individuals, or both. Civil penalties may be imposed administratively in amounts up to $11,000 per violation. The E.O. provides the domestic legal basis to implement the obligations to freeze the assets of individuals and entities listed pursuant to UNSCRs 1267, 1333, 1390 and 1455. This authority is further detailed in the USG report to the 1373 Counter-Terrorism Committee (See also S/2001/1220 pages 6-9, 11).

USA PATRIOT Act – The USA PATRIOT Act enhances information sharing ability between and among various financial, law enforcement, legal, and intelligence communities on terrorism financing issues. The PATRIOT Act also enhances the regulation of non-banking services. (See also S/2001/1220, page 4.)

IEEPA – Provides the President with certain specified powers to regulate the property and interests in property of, or economic relations with, foreign persons to respond to a national emergency declared with respect to any unusual and extraordinary threat, which has as its source in whole or substantial part outside the United States, to the national security, foreign policy or economy of the United States.

United Nations Participation Act (UNPA) - Section 5 of the UNPA, 22 U.S.C. § 287c, authorizes the President to give effect domestically to mandatory measures decided upon by the Security Council pursuant to Article 41 of the UN Charter. Section 5 specifically authorizes the President to regulate, by
Executive Order, economic relations within the United States and between the United States and any foreign country. This provision thus provides authority for the President to implement economic sanctions decided on by the UN Security Council.

Section 219 of the Immigration and Nationality Act (INA), as amended, and related provisions - Pursuant to this statutory provision, the Secretary of State, in consultation with the Secretary of the Treasury and the Attorney General, has the authority to designate foreign organizations that satisfy certain specified criteria as foreign terrorist organizations (FTO). (See 8 U.S.C. § 1189.) There are currently 36 organizations designated by the Secretary of State as FTOs. For FTOs, any U.S. financial institution that becomes aware that it has possession of or control over the funds in which an FTO has an interest is required to retain control of or control over those funds and report the funds to OFAC. Members and representatives of an FTO, if they are alien, are inadmissible to and, in certain circumstances, removable from the United States.

Section 2339B of the U.S. Criminal Code (Title 18 of the U.S. Code) – This Section makes it illegal for persons within the United States or subject to U.S. jurisdiction to knowingly provide, or attempt or conspire to provide, "material support or resources" to FTOs designated pursuant to section 219 of the INA, an amended. This statute has been used to prosecute persons who have provided material support or resources to designated FTOs including Al Qaida, the Palestinian Islamic Jihad, Gama'a al-Islamiya, and Hizballah. It has also been applied against persons who plotted to provide weaponry to terrorist organizations in exchange for narcotics, and person who have provided terrorist groups with funds derived from illegal activity. It has also been applied against persons who plotted to provide weaponry to terrorist organizations in exchange for narcotics, and person who have provided terrorist groups with funds derived from illegal activity. Penalties for violations of Section 2339B include fines and/or imprisonment for up to 15 years or, if the death of any person results, life imprisonment or the death penalty.

Civil Forfeiture Law - The United States has the authority to seize all assets, foreign or domestic, of any individual, entity or organization engaged in planning or perpetrating any act of international or domestic terrorism against the United States, its citizens and residents, or their property, and all assets, foreign or domestic, affording any person a source of influence over any such entity or organization, or all assets acquired or maintained by any person for the purpose of supporting, planning, conducting, or concealing such terrorist acts, or derived from, involved in, or used or intended to be used in the commission of such terrorist acts {18 U.S.C. § 981(a)(1)(G)}.

The civil forfeiture actually results in the permanent transfer of ownership of the assets to the United States. Forfeiture actions are judicial in nature, initiated by the Department of Justice, and subject to adversarial proceedings.

Banking Secrecy Act (BSA) - The Currency and Foreign Transactions Reporting Act, also known as the Bank Secrecy Act (BSA), and its implementing regulation, Title 31 Code of Federal Regulations (CFR), Part 103, are tool the USG uses to fight drug trafficking, money laundering, and other crimes. Congress enacted the BSA to prevent banks and other financial service providers from being used as intermediaries for, or to hide the transfer or deposit of money derived from, criminal activity. The original focus of the BSA was on banks, which are the main financial institutions that deal in cash. To protect the U.S. financial system from criminal activity and to promote the detection and prosecution of financial crimes, Congress added anti-money laundering provisions to the BSA in 1992, which authorized Treasury to apply the law to many different types of financial institutions.

Coordination

The USG has taken steps to coordinate the various intelligence, law enforcement, regulatory, and diplomatic agencies to bring the appropriate actions to bear against the various terrorism financing targets. The following bodies are responsible for coordinating on various levels:

The Terrorism Financing Policy Coordination Committee (PCC), established under the directive of the NSC and chaired by Treasury, directs and coordinates the interagency efforts to understand and disrupt terrorism financing networks.

Department of State – Coordinates bilaterally and multilaterally with other governments to freeze the assets of terrorists and their supporters, including those of Usama bin Laden, Al Qaida and the Taliban, and their associates. These international efforts are coordinated on an inter-agency basis in Washington and with U.S. diplomatic posts abroad.

Operation Green Quest - Operation Green Quest is an interagency law enforcement body led by the Bureau of Immigration and Customs Enforcement (ICE) created to identify, disrupt, and dismantle the organizations and systems that serve as sources of terrorist funding. Through a broad systematic strategy, the combined statutory authorities of its representative member agencies and its command and control center, OGQ follows suspicious financial activities that may be indicative of terrorist-finance, as well as financial and trade systems that are susceptible to exploitation by terrorist financiers.

EOTF/FC – Treasury's Executive Office for Terrorist Financing and Financial Crimes provides policy oversight to FinCEN and OFAC, and leads USG efforts in developing and ensuring global compliance with international standards on terrorism financing through the Financial Action Task Force (FATF).

TFTF – Treasury's Task Force on Terrorist Financing monitors and tracks countries' efforts to combat the financing of terrorism and works bilaterally, regionally, and multilaterally to strengthen international efforts.

11. Please convey the steps banks and/or other financial institutions are required to take to locate and identify assets attributable to, or for the benefit of, Usama bin Laden or members of Al Qaida or the Taliban, or associated entities or individuals. Please describe any "due diligence" or "know your customer" requirements (Footnote 2: For details see Third Report of the Monitoring Group of 17 December 2002/1338, Chapter V. paragraphs 27-29). Please indicate how these requirements are enforced, including the names and activities of agencies responsible for oversight.

Under E.O. 13224 the assets of individuals and entities designated as Specially Designated Global Terrorists (SDGTs), published by OFAC are frozen and all persons in the United States and U.S. persons, wherever located, including financial institutions, are prohibited from engaging in transactions or dealings with SDGTs. While each financial institution must comply with E.O. 13224, financial institutions may differ in their approaches to locating and identifying assets. Compliance programs are tailored to individual institutions, and these financial institutions often consult with OFAC in implementing these programs. Many use interdiction software. This software enables users to locate and identify assets held by targets as well as assets in sanctioned countries. Any person within U.S. jurisdiction found not to have blocked the assets of, or to have dealt with, an individual or entity on OFAC's SDGT list is subject to severe civil and/or criminal penalties. Information on potential violations comes to OFAC's attention through a variety of sources, including reports filed by banks, which have blocked funds, and through other law enforcement agencies.

12. Resolution 1455 (2003) calls on Member States to provide "a comprehensive summary of frozen assets of listed individuals and entities." Please provide a list of the assets that have been frozen in accordance with this resolution. This list should also include assets frozen pursuant to resolutions 1267 (1999), 1333 (2001) and 1390 (2002). Please include, to the extent possible, in each listing the following information:

- **identification(s) of the person or entities whose assets have been frozen;**
- **a description of the nature of the assets frozen (i.e., bank deposits, securities, business assets, precious commodities, works of art, real estate property, and other assets);**
- **the value of assets frozen.**

Since September 11, 2001 the United States has frozen a total of $36.3 million in 102 accounts of terrorists and terrorist supporters. Of this amount, the United States has frozen $3.24 million in Al Qaida-related assets and originally froze $26.64 million in Taliban-related assets within U.S. jurisdiction. The following is a summary of assets frozen of individuals and entities on the UN 1267 Sanctions Committee consolidated list within the United States or within the possession or control of U.S. persons.

Taliban - The United States froze $26.64m in 24 accounts of Afghan-government assets that had been linked to the Taliban in September and October 2001. All of these Afghan-government assets were subsequently unfrozen in January and February 2002 and restored to the Afghan government after the Taliban no longer controlled any territory within Afghanistan;

Al Barakaat - The United States froze $1,209,000 in 38 accounts pursuant to the November 7, 2001, designation of al Barakaat-related entities. Of that amount, $679,000 in 14 accounts was unfrozen pursuant to the August 27, 2002, delisting of 4 U.S.-based entities that had been linked to the al Barakaat network;

Global Relief Foundation - The United States froze $1,0215,000 in 6 accounts pursuant to the October 18, 2002, designation of the Global Relief Foundation and pursuant to the December 14, 2001, blocking of the Global Relief Foundation's accounts in aid of investigation;

Benevolence International Foundation - The United States froze $914,000 in 7 accounts pursuant to the November 19, 2002, designation of the Benevolence International Foundation and pursuant to the December 14, 2001, blocking of the Benevolence International Foundation's accounts in aid of investigation;

Lajnat al Daawa al Islamiyya - The United States froze $105,000 pursuant to the January 9, 2003 designation of Lajnat al Daawa al Islamiyya (the Islamic Call Committee).

13. Please indicate whether you have released pursuant to resolution 1452 (2002) any funds, financial assets or economic assets that had previously been frozen as being related to Usama bin Laden or members of the Al Qaida or the Taliban or associated individuals or entities. If so, please provide reasons, amounts unfrozen or released and dates.

The USG has authorized access to $2.2 million for basic living expenses and reasonable professional fees of persons whose assets are frozen pursuant to E.O. 13224.

14. Pursuant to resolutions 1455 (2003), 1390 (2001), 1333 (2000) and 1267 (1999), States are to ensure that no funds, financial assets or economic resources are made available, directly or indirectly, to Listed individuals or entities or for their benefit, by nationals or by any persons within their territory. Please indicate the domestic legal basis, including a brief description of laws, regulations and/or procedures in place in your country to control the movements of such funds or assets to designated individuals and entities. This section should include a description of:

- **The methodology, if any, used to inform banks and other financial institutions of the restrictions placed upon individuals or entities listed by the Committee, or who have otherwise been identified as members or associates of Al Qaida or the Taliban. This section should include an indication of the types of institutions informed and the methods used.**

- **Required bank-reporting procedures, if any, including the use of Suspicious Transaction Reports (STR), and how such reports are reviewed and evaluated.**

- **Requirements, if any, placed on financial institutions other than banks to provide STRs, and how such reports are reviewed and evaluated.**

- **Restrictions or regulations, if any, placed on the movement of precious commodities such as gold, diamonds and other related items.**

- **Restrictions or regulations, if any, applicable to alternate remittance systems such as -- or similar to – "hawala", as well as on charities, cultural and other non-profit organizations engaged in the collection and disbursement of funds for social or charitable purposes.**

(See also answer to Question 2 on the domestic legal basis in the United States for controlling the movement of funds or assets of designated individuals and entities.)

The financial community is informed of additions to the list of Specially Designated Global Terrorists in a variety of ways. OFAC has automated its compliance notifications. There are currently over 10,000 subscribers to a special Listserv E-mail notice system connected to OFAC's website providing instant updates on important sanctions information to the financial community. OFAC also sends individual electronic updates to well over 5,000 U.S. financial institutions through the clearinghouse interbank payments system and through central banking facilities in the United States. Key industry groups and regulators receive individual notices via both facsimile and E-mail. In addition to its website, OFAC also maintains a 24/7 fax-on-demand service, which is immediately updated as changes occur. Finally, OFAC maintains a toll-free telephone "hotline" to address sanctions issues.

All parties freezing property or rejecting financial transactions are required to report those actions in writing to OFAC within ten business days. Every U.S. person holding frozen assets must also file an annual report with OFAC on that frozen property.

Moreover, the BSA, codified at 31 U.S.C. § 5311 et seq., authorizes the Secretary of the Treasury to issue regulations requiring banks to keep records and file reports that are determined to have a high degree of usefulness in criminal, tax and regulatory investigations or proceedings, or in the conduct of intelligence or counter-intelligence activities to protect against international terrorism, and to implement anti-money laundering compliance programs and compliance procedures. Regulations implementing the BSA appear at 31 CFR Part 103. The authority to administer the BSA has been delegated to the Director of FinCEN.

Prior to the enactment of the USA PATRIOT Act, regulations applying the anti-money laundering provisions of the BSA were issued only for banks and certain other institutions that offer bank-like services or that regularly deal in cash. These regulations require such financial institutions to take the following actions: (1) Keep records related to certain monetary instrument purchases and funds transfers; (2) Report currency transactions of more than $10,000 by, through, or to the financial institution; (3) Report the transport of currency across U.S. borders; (4) Report certain accounts that United States citizens and residents hold at foreign financial institutions; and (5) Report suspicious transactions relevant to possible violations of the law.

Title III of the USA PATRIOT Act amends the BSA to make it easier to prevent, detect, and prosecute international money laundering and the financing of terrorism by: (1) Requiring that every financial institution establish an anti- money laundering program that includes, at a minimum, (i) the development of internal policies, procedures, and controls; (ii) the designation of a compliance officer; (iii) an ongoing employee training program; and (iv) an independent audit function to test the program; (2) Requiring Treasury to prescribe, jointly with the identified federal financial regulators, regulations setting forth minimum standards regarding the verification of the identity of any person seeking to open an account; (3) Requiring each U.S. financial institution that establishes, maintains, administers, or manages a private banking account or correspondent account in the United States for a non-U.S. person to take certain anti- money laundering measures with respect to such accounts; (4) Prohibiting certain financial institutions from establishing, maintaining, administering, or managing a correspondent account in the United States for a foreign shell bank (other than certain foreign shell banks with regulated affiliates); and (5) Permitting financial institutions, their regulatory authorities, and law enforcement authorities to share information regarding persons engaged or reasonably suspected, based on credible evidence, of engaging in terrorist acts or money laundering activities.

The USA PATRIOT Act required the extension of the anti-money laundering program requirements to financial institutions, such as investment companies, that had not previously been subjected to BSA regulations, and added new entities to the statutory definition of financial institution, such as futures commission merchants, commodity trading advisors, and commodity pool operators.

FinCEN receives Suspicious Activity Reports (SARs), filed by depository institutions (i.e., banks, thrifts, savings and loans, and credit unions), money services businesses (i.e., money transmitters and travellers checks and money order issuers) and broker-dealers. Among other purposes FinCEN examines the SAR database to determine the extent to which SARs have been filed relating to terrorism. Twice a year, FinCEN publishes a report, The *SAR Activity Review-Trends, Tips and Issues* to provide meaningful information about the preparation, use, and value of SARs filed by financial institutions.

FinCEN regularly publishes *SAR Bulletins*, which are reports based on information drawn from the Suspicious Activity Reporting System to alert financial institutions to trends and patterns in money laundering and terrorist financing. The most recent issue, published in January 2002, reports on financial transactions indicative of terrorist funding. FinCEN also publishes Advisories that provide guidance to financial institutions in monitoring and reporting suspicious transactions. Most recently, FinCEN published an Advisory relating to Informal Value Transfer Systems.

Federal, state and local law enforcement agencies have direct electronic access to all BSA reports, and can use them to support ongoing investigations and as leads. In addition, FinCEN provides assistance to law enforcement investigations on request and proactively by analyzing the BSA database looking for connections and patterns to illegal activity, especially the financing of terrorism.

Finally, pursuant to its regulation issued under Section 314 of the U.S.A. PATRIOT Act, FinCEN transmits to financial institutions target lists of persons suspected by federal law enforcement agencies of terrorist financing or money laundering. Financial institutions are required to search their records for accounts or transactions involving these targets and report match to FinCEN the existence of any matches. FinCEN then combines all the responses and provides them to law enforcement for follow up with appropriate legal process.

In addition to banks, the regulations (31 CFR §§ 103.18, 103.19, and 103.21) implementing a provision of the BSA (31 U.S.C. § 5318(g)) require the following persons and entities to file suspicious activity reports:

- Thrifts, savings & loan associations, and credit unions (which the regulations define as "banks");
- Money transmitters, issuers/sellers/redeemers of traveler's checks, and money orders;
- The United States Postal Service;
- Broker-dealers (31 CFR § 103.19);
- Casinos (31 CFR § 103.21(g)) (as of March 25, 2003); and
- Currency dealers and exchangers (effective August 11, 2003).

Further, FinCen has proposed imposing SAR requirements on mutual funds and life insurance companies. These proposed regulations are in the process of being finalized. In addition, Treasury presented reports to Congress concerning the regulation of commodities brokers and investment companies pursuant to 31 U.S.C. § 5318 as directed by section 356 of the USA PATRIOT Act. Further actions are under review.

FinCen has issued a proposed rule to prescribe minimum standards applicable to dealers in precious metals, stones, or jewels pursuant to the provisions in the USA PATRIOT Act, which requires financial institutions to establish anti-money laundering programs. The rule has been published for comment, 68 Federal Register 8480 (February 21, 2003).

Under the USA PATRIOT Act, the USG has taken steps to regulate and register informal value transfer systems (IVTS), also known as hawalas or alternative remittance systems. The USA PATRIOT Act expanded the definition of "financial institution" to include IVTS operators. As such, they now must comply with all BSA registration, record keeping, reporting and anti-money laundering program requirements.

Section 5330 of the BSA and FinCEN's implementing regulations require all money transmitting businesses (but not their agents) to register with FinCEN. Section 1960 of Title 18 makes it a felony to operate an unlicensed money transmitting business. Additionally, a money transmitting business that fails to register with FinCEN as a money services business (MSB) is operating as an unlicensed money transmitter with penalties to include civil and criminal fines, imprisonment, or both.

An explanation of how the USG regulates fundraising and activities of non-profit organizations and charities is detailed in UNSC S/2002/674, pages 9-17.

IV. TRAVEL BAN

Under the sanctions regime, all States shall take measures to prevent the entry into or transit through their territories of Listed Individuals (paragraph 1 of resolution 1455 (2003), paragraph 2b of resolution 1390 (2002)).

15. Please provide an outline of the legislative and/or administrative measures, if any, taken to implement the travel ban.

The United States has enacted legislation, promulgated executive orders, and taken other administrative measures to strengthen its immigration laws and related measures relative to the transit of listed individuals. The USA PATRIOT Act effected five major changes to existing U.S. immigration laws (8 U.S.C. § 1101 et seq.) that are pertinent:

1. It created five new categories of aliens who are to be excluded from entering the United States:

A. representatives of groups that endorse terrorism, if the Secretary of State finds that activity undermines U.S. counter-terrorism efforts;

B. aliens who use their prominence to persuade others to commit terrorism, if the Secretary of State finds that activity undermines U.S. counter-terrorism efforts;

C. aliens who associated with terrorist groups, who the Secretary of State or Attorney General find seek to enter the United States to endanger U.S. security;

D. terrorists' spouses and children; and

E. money launderers;

2. It revised the "terrorist activity" definition in 8 U.S.C. § 1182(a)(3)(B) to include the use of any "other weapon or dangerous device," (e.g., knives and other edged weapons) with intent to endanger the safety of one or more individuals or to cause substantial damage to property;

3. It expanded "terrorist organization" for immigration and other purposes to include:

A. designated FTOs under 8 U.S.C. § 1189 (triggers criminal, immigration, financial asset sanctions);

B. other designated organizations which commit or incite to commit, under circumstances indicating an intention to cause death or serious bodily injury, a terrorist activity; prepare or plan a terrorist activity; gather information on potential targets for terrorist activity; or provide material support to further terrorist activity (triggers immigration sanctions only);

C. other groups of two or more individuals, whether organized or not, which engage in certain terrorist activity (triggers immigration sanctions only);

4. It revised the terrorism material support criteria in existing U.S. law to include soliciting members, funds or other things of value, or providing support for terrorist activity, terrorists, or terrorist organizations.

5. It provided new detention authority to the U.S. Attorney General (AG). If the AG certifies that there are reasonable grounds to believe an alien is described in the immigration law's removal provisions for espionage and sabotage, export controls violations, overthrow of the United States, terrorism, or "is engaged in any other activity that endangers the national security," that alien may be detained.

16. Have you included the names of the listed individuals in your national "stop list" or border checkpoint list? Please briefly outline steps taken and any problems encountered.

Not all names of listed individuals have been included in national lists accessed by Customs & Border Protection due to the lack of biographical data and hard information that can be used to exclude individuals from entry into the United States. CBP access all names that are in the State Department Tipoff Program as the main source of data to determine excludability. CBP also uses the names of listed individuals to establish alerts and lookouts for company import and export activity. Lookouts are established in enforcement databases, which are screened at time of import/export to determine targets for additional screening and examination. When biographical data is not included with a listed

individual, CBP conducts research to establish possible suspects or names beyond the original listed individuals. The expansion of the subject list to included additional biographical information would greatly improve CBP's ability to target suspect individuals.

Also see answers under questions 2 and 3 above.

17. How often do you transmit the updated List to your border control authorities? Do you possess the capability of searching List data using electronic means at all your entry points?

Suspect lists and lookouts reside within enforcement databases (eg. Tipoff, IBIS, NAILS and TECS) which are queried when a passenger or cargo enters the United States. These lists and lookouts are updated whenever information is received. Customs and Border Protection Office of Intelligence coordinates this effort by querying existing databases and establishing new records where previous records do not exist. CBP employees have the ability to electronically access these lists at every port of entry into the United States.

Also see answers under questions 2 and 3 above.

18. Have you stopped any of the listed individuals at any of your border points or while transiting your territory? If so, please provide additional information, as appropriate.

Customs and Border Protection can state that on this list of individuals belonging to or associated with Al-Qaida, CBP intercepted Youssef Mustafa Nada (DOB 05/17/37)(#69,pg 18). The subject attempted to enter the United States in Atlanta on 12/08/99. He arrived on Swissair flight 120 and was in possession of an Italian passport. He sought admission as a visa waiver applicant and was denied entry. The FBI was notified.

See answer under question 3 above. In addition, USG policy is not to comment on pending enforcement or litigation matters.

19. Please provide an outline of the measures, if any, taken to incorporate the List in the reference database of your Consular offices. Have your visa-issuing authorities identified any visa applicant whose name appears on the List?

See answer under question 3 above. In addition, USG policy is not to comment on pending enforcement or litigation matters.

V. ARMS EMBARGO

Under the sanctions regime, all States are requested to prevent the direct or indirect supply, sale and transfer, to Usama bin Laden, members of Al Qaida organization and the Taliban and other individuals and entities associated with them, from their territories or by their nationals outside their territories of arms and related materiel of all types, including the provision of spare parts and technical advice, assistance, or training related to military activities (paragraph 2(c) of resolution 1390 (2002) and paragraph 1 of resolution 1455 (2003)).

20. What measures, if any, do you now have in place to prevent the acquisition of conventional arms and weapons of mass destruction (WMD) by Usama bin Laden, members of Al Qaida organization and the Taliban and other individuals, groups, undertakings and entities associated with them? What kind of export control do you have in place to prevent the above targets from obtaining the items and technology necessary for weapons development and production?

The U.S. munitions export control system is designed to deny adversaries and parties whose interests are inimical to those of the United States access to U.S.-origin defense equipment and technology. This function is administered by the

Directorate of Defense Trade Controls (DDTC), U.S. Department of State. Its primary missions, in accordance with the Arms Export Control Act (AECA) and the International Traffic in Arms Regulations, include:

(a) Regulating, in furtherance of U.S. national security and foreign policy objectives, commercial transfers of defense articles and defense services covered by the United States Munitions List;

(b) Administering and enforcing arms export control law and regulations; and

(c) Providing regulatory and foreign policy guidance to persons involved in the manufacture, brokering and export of defense articles, and provision of defense services, consistent with U.S. law and policy.

As a matter of long-standing policy, rooted in law, the United States is fully cognizant of the potentially adverse consequences of indiscriminate arms transfers and, therefore, strictly regulates exports and re-exports of defense items and technologies to protect its national interests and those interests in peace and security of the broader international community.

In addition to seeking technical support and national security assessments from the Department of Defense, the State Department relies on extensive interagency cooperation and coordination to perform the arms export control function. It:

-- Works closely with U.S. Customs (review of defense industry registration, performance of defense export end-use checks, investigations, civil penalties);

-- Also works with the Intelligence Community to review alleged diversions and unauthorized transfers; and

-- Cooperates with the Justice Department and U.S. Attorneys (pre-trial consultations, trial documentary preparation, expert testimony).

Moreover, in accordance with the AECA, registration with the State Department (via DDTC) of all U.S. persons that manufacture or export defense articles, furnish defense services, or U.S. and foreign persons engaged in arms brokering, is required. The information submitted by registrants is reviewed by the Treasury Department to ensure there are no outstanding law enforcement concerns. Registration does not confer any export privileges, but is a prerequisite to export licensing approval.

The registration process:

-- Informs the USG about U.S. defense industry (legal status, export eligibility, foreign ownership/affiliations, legally responsible personnel, areas of activity);

-- Serves as a channel to provide industry information about export regulations and government concerns; and

-- Helps validate the bona fides of U.S. firms engaged in defense trade, especially during the review of export license applications.

Department of State approval of a license application is required prior to the export of defense articles or defense services. During the review process, a computerized review of all parties to the proposed transactions is made against a "Watch List" of known or suspected export violators. A "match" results in a full compliance review by the State Department before final action is taken on the application. Usama bin Laden, members of Al Qaida and the Taliban, and other individuals and entities that have been identified by the USG as being associated with them are included on the Watch List.

In addition to sorting through detailed technical specifications regarding munitions and weapons systems, the license application review process clarifies the ultimate end-use and end-user of the defense export, as well as facts related to intermediate handling. This process is designed to detect whether parties ineligible to participate in defense trade (e.g., Usama bin Laden, Al Qaida members, and associates) would benefit directly or indirectly from the proposed export transaction.

From the enforcement point of view, the review process provides an avenue to prevent or eliminate diversions, and to assist the USG in investigations and prosecutions should an export violation be suspected or reported.

End-Use Checks are key to the State Department's effort to prevent illegal defense exports and technology transfers. Implemented under the program name "Blue Lantern," these checks enlist the help of foreign governments and private sector parties in the conduct of pre-license checks and post-shipment verifications of defense exports. The scope of the inquiry might range from simple contacts to verify the bona fides of a transaction to physical inspection of an export.

21. What measures, if any, have you adopted to criminalize the violation of the arms embargo directed at Usama bin Laden, members of Al Qaida organization and the Taliban and other individuals, groups, undertakings and entities associated with them?

Pursuant to the AECA, arms export control violations, including provision of defense equipment and technology to ineligible persons, such as bin Laden, Al Qaida members, the Taliban, and associated persons, are subject to strict criminal and civil penalties. Criminal penalties may include a jail sentence of 10 years and/or $1 million for each violation. Possible civil penalties include debarment from participation in U.S. defense trade and monetary penalties up to $500,000 per violation.

On October 24, 2002, the Department of State published in the Federal Register a list of persons that are subject to an arms embargo under UNSCR 1390 (continued in UNSCR 1455). The list includes Usama bin Laden, and persons associated with the Taliban and Al Qaida. Violation of this embargo would most likely be investigated by the U.S. Customs Service, which would bring such investigations to the attention of an Assistant U.S. Attorney for possible criminal prosecution.

22. Please describe how your arms/arms broker licensing system, if any, can prevent Usama bin Laden, members of Al Qaida organization and the Taliban and other individuals, groups, undertakings and entities associated with them from obtaining items under the established arms embargo.

U.S. regulation of arms brokering activity covers a broad range of activity. Law and regulations seek to ensure that U.S. persons and foreign persons subject to U.S. jurisdiction do not participate in or benefit from munitions export activity subject to embargoes and other arms trade sanctions.

The AECA requires registration of any person "who engages in the business of brokering activities." U.S. regulations define brokering activities to include "the financing, transportation, freight forwarding, or taking of any other action that facilitates the manufacture, export, or import of a defense article or defense service, irrespective of its origin."

Under U.S. law, "no person may engage in the business of brokering activities" without a license. Pursuant to this law, persons subject to U.S jurisdiction would be denied approval to engage in brokering activities that would support or assist Usama bin Laden, Al Qaida, the Taliban, and associated persons.

23. Do you have any safeguards that the weapons and ammunition produced within your country will not be diverted/used by Usama bin Laden, members of Al Qaida organization and the Taliban and other individuals, groups, undertakings and entities associated

Providing foreign access to U.S. defense equipment and technology, whether in the United States or abroad, constitutes an export that is subject to explicit USG approval.

As indicated above, this export control process is closely regulated and excludes the participation of embargoed and other ineligible parties in U.S. defense trade.

Exports are recorded in the Automated Export System (AES), which is monitored by the Bureau of Customs & Border Protection (CBP) and the Census Bureau. CBP reviews all export data submitted through AES and targets suspect shipments for enforcement examination. CBP's Automated Targeting System -- Anti-Terrorism (AES-AT) -- electronically checks all AES data against enforcement databases. Automated holds are placed on any export shipments that have a positive match for suspects listed on watch-lists. Cargo placed on hold cannot be exported prior to examination and release by CBP.

VI. ASSISTANCE AND CONCLUSION

24. Would your state be willing or able to provide assistance to other States to help them implement the measures contained in the above-mentioned resolutions? If so, please provide additional details or proposals.

Building the capacity of our coalition partners to combat money laundering and terrorist financing through cooperative efforts, and through training and technical assistance programs is critical to our national security. The United States is a provider of technical assistance in a wide variety of counter-terrorism areas. This information has been previously provided in detail to the UN Counter-Terrorism Committee overseeing implementation of UNSCR 1373. What follows below is an overall description of the United States' technical assistance efforts.

While there are some important differences between money laundering and terrorist financing, in terms of capacity building through training and technical assistance there is no appreciable difference. The same measures that are used to prevent, detect, investigate and prosecute money laundering -- sound legislation and regulations, suspicious transaction reporting mechanisms, Financial Intelligence Units, on-site supervision of the financial sector, internal controls, trained financial investigators, legal authorization to utilize special investigative techniques, modern asset forfeiture and administrative blocking capability, and the ability to cooperate and share information internationally -- are precisely the tools required to identity, interdict and disrupt terrorist financing.

While significant progress is being made, additional efforts are still necessary to secure expertise, devote resources to training and technical assistance, prioritize requirements, and then harmonize assistance efforts to continue the headway made thus far against money laundering and terrorist financing.

Shortly after September 11, 2001, the Department of State convened an interagency group to identify those countries most vulnerable to terrorist financing and to devise a strategy to provide them with the necessary training and technical assistance to create comprehensive, effective anti-money laundering/anti-terrorist financing regimes. Throughout 2002, State Department-led Financial Systems Assessment Teams (FSATs) of U.S. experts conducted detailed assessments of the legal, regulatory and law enforcement capabilities and vulnerabilities of the most affected countries. By the end of the year, a majority of these countries had been assessed. Training and technical assistance implementation plans had been developed on virtually all of the assessed countries, and assistance had begun being delivered according to these plans. This program remains a high priority in 2003 and will be pursued until comprehensive anti-money laundering regimes are established in all of the priority countries.

Department of State

Through the Department of State's Bureau for International Narcotics and Law Enforcement Affairs (INL), in close coordination with the Department's Office of the Coordinator for Counter-Terrorism on terrorist financing issues, $3.27

million was expended in fiscal year 2002 to provide law enforcement, prosecutorial and central bank training to countries around the globe. A prime focus of the training program was a multi-agency approach to develop or enhance financial crime and anti-money laundering regimes capable of combating not only money laundering activities but also terrorist financing in selected jurisdictions. Supported by and in coordination with the State Department, several government and non-government organizations offered law enforcement, regulatory and criminal justice programs worldwide.

During 2002, 37 INL-funded programs were delivered in 31 countries to combat international financial crimes, money laundering and terrorist financing. Nearly every federal law enforcement agency assisted in this effort by providing basic and advanced training courses in all aspects of financial criminal activity. In addition, INL made funds available for intermittent posting of financial advisors at selected overseas locations to work directly with host governments to assist in the creation, implementation, and enforcement of anti-money laundering and financial crime legislation. INL also provided several federal agencies funding to conduct multi-agency financial crime training assessments and develop specialized training in specific jurisdictions worldwide to combat money laundering.

INL, along with the European Union and the Government of the United Kingdom, continues to fund the Caribbean Anti-Money Laundering Programme (CALP). Its objectives are to reduce the laundering of the proceeds of all serious crime by facilitating the prevention, investigation, and prosecution of money laundering and to develop a sustainable institutional capacity in the Caribbean region to address the issues related to anti-money laundering efforts at local, regional and international levels.

In 2002, INL contributed to the United Nations Global Program Against Money Laundering (GPML). The GPML sponsored money-laundering conferences, provided short-term training courses, and instituted a unique longer-term technical assistance initiative through its mentoring program. The mentoring program provides advisors on a yearlong basis to specific countries or regions.

INL continues to provide significant financial support for many of the anti-money laundering bodies around the globe. During 2002, INL furnished support to the Financial Action Task Force on Money Laundering (FATF) and to FATF-styled regional bodies, including the Asia/Pacific Group on Money Laundering, the Council of Europe's Moneyval, formerly known as the Select Committee of Experts on the Evaluation of Anti-Money Laundering Measures, and the Caribbean Financial Action Task Force. INL also provided financial support to the evolving ESAAMLG (Eastern and Southern African Anti-money Laundering Group), and the South American Financial Action Task Force (Grupo de Accion Financiera de Sudamerica Contra el Lavado de Activos) the FATF-styled regional body in South America.

International Law Enforcement Academies (ILEAs)

The ILEAs are a progressive concept in the area of international assistance programs. These academies offer a core law enforcement management program, regional seminars, and specialized training programs tailored to region-specific needs and emerging global threats, such as terrorism. The Department of State works with the Departments of Justice and Treasury, and with foreign governments to implement the ILEA programs. To date, the combined ILEAs have trained over 10,000 officials from 50 countries. The ILEAs are located in Budapest, Hungary; Bangkok, Thailand; Gaborone, Botswana; and Roswell, New Mexico. A fifth ILEA is being planned in San Jose, Costa Rica.

Board of Governors of the Federal Reserve System (FRB)

The FRB is active in the effort to deter money laundering, primarily through ensuring compliance with the Bank Secrecy Act and the USA PATRIOT Act by the domestic and foreign banking organizations that it supervises. FRB staff also conducted training in anti-money laundering tactics and provided technical assistance to banking supervisors and law enforcement officials throughout the world. Programs for Malaysia, Dominican Republic, Argentina, Barbados, Turkey, and the Philippines were provided in 2002. The FRB also participated in financial sector assessment trips to several countries in the Middle East as a member of U.S. interagency teams.

Drug Enforcement Administration (DEA)

The DEA Office of Training, International Training Section, conducts the International Asset Forfeiture and Money Laundering Seminar portions of the Department of Justice in-country Asset Forfeiture Program. Approximately 35 foreign government officials attend each seminar. The Department of Justice, the U.S. Customs Service, the U.S. Marshal Service, and various divisional offices of DEA provide the guest lecturers. The course curriculum includes instruction addressing money laundering and its relation to central bank operations, asset identification, seizure and forfeiture techniques, financial investigations, document exploitation, and international banking. Overviews of U.S. asset forfeiture law, country forfeiture and customs law, and prosecutorial perspectives are also included. In 2002, seminars were conducted in Germany, Guatemala, Ecuador, Netherlands, Dominican Republic, and the United Kingdom.

Federal Bureau of Investigation (FBI)

During 2002, FBI agents and analysts assigned to the Terrorist Finance Operations Section (TFOS) provided training and presentations relating to terrorism financing methods and money laundering to law enforcement and banking officials of Australia, Belgium, Canada, Germany, Kuwait, the Netherlands, New Zealand, Finland, Germany, Jordan, Paraguay, Pakistan, Philippines, Russia, Singapore, Switzerland, Turkey, Thailand, United Arab Emirates and the United Kingdom. Additional course instruction was also provided on topics ranging from evidence acquisition and case organization to computer forensic examination techniques. In November 2002, TFOS sponsored an international seminar on the informal value transfer system hawala. Officials from India, Pakistan, Jordan, and the United Kingdom attended this weeklong conference.

Federal Deposit Insurance Corporation (FDIC)

The FDIC participated in the conduct of assessments of the vulnerabilities to terrorist financing of Pakistan and Malaysia and developed and implemented appropriate technical assistance plans. Working collaboratively with anti-money laundering experts from Malaysia and New Zealand, the FDIC evaluated Fiji's compliance with the FATF Forty Recommendations on Money Laundering and participated in a review of Pakistan.

The FDIC's participated in the decision-making process of the Basel Committee that led to the April 17, 2002 issuance of the Sharing of Financial Records Between Jurisdictions in Connection with the Fight Against Terrorist Financing.

FDIC staff meets with foreign government representatives to discuss anti-money laundering and related regulatory issues, including examination policies and procedures, the FDIC's asset forfeiture programs, suspicious activity reporting requirements and interagency information sharing mechanisms. In 2002, such presentations were given to Antigua, Barbados, Brazil, Chile, Dominica, Grenada, Russia, St. Lucia, St. Vincent and the Grenadines, and Thailand.

In April 2002, the FDIC sponsored the FDIC International Visitors Training Program. In addition to sessions on deposit insurance, bank closing procedures and general supervisory issues, international conventions and specific requirements of the USA PATRIOT Act that will affect the international community were addressed. Attendees represented Armenia, Bosnia and Herzegovina, Bulgaria, Canada, China, Czech Republic, Estonia, Germany, Hong Kong, Hungary, Indonesia, Japan, Mozambique, Serbia, Thailand, Turkey and Venezuela.

FDIC provided anti-money laundering training and technical assistance to the Republic of the Marshall Islands (RMI) in 2002. FDIC assisted RMI in developing anti-money laundering regulations and examination procedures. The RMI had been on the FATF NCCT list, and the U.S. Treasury Department had issued financial advisories to U.S. banks warning them to scrutinize RMI transactions. Among the deficiencies cited by FATF was the lack of a regulatory scheme to detect money laundering in financial institutions.

In September 2002, FDIC staff gave an anti-money laundering presentation to the Taiwan Academy of Banking and Finance, a group comprised of various banking supervisory agencies. Topics included the Bank Secrecy Act, the USA PATRIOT Act, components of anti-money laundering examination programs and procedures, and an effective bank anti-money laundering program.

Financial Crimes Enforcement Network (FinCEN)

FinCEN, the U.S. Financial Intelligence Unit (FIU) coordinates and provides training and technical assistance on financial crimes, anti-money laundering regulatory regimes, and establishing Financial Intelligence Units. FinCEN's international training program has two main components: (1) instruction to a broad range of government officials on money laundering and FinCEN's mission and operation; and (2) financial intelligence analysis training and the operational aspects of FIUs. FinCEN works closely with other members of the Egmont Group of FIUs to provide training and technical assistance to various jurisdictions in establishing and operating their own FIUs.

During 2002, FinCEN conducted training courses independently, as well as with other agencies. Such training sessions were held in Bulgaria and Poland in 2002.

Much of FinCEN's work also involves strengthening existing FIUs and reinforcing channels for communicating operational information, including participation in personnel exchanges, e.g., weeklong exchanges with the FIUs of Turkey and South Korea, and regional and operational workshops. For instance FinCEN hosted a workshop on Informal Value Transfer Systems (IVTS) in Mexico in October 2002 that included presentations and discussions about the money laundering risks posed by IVTS service providers, and the law enforcement and regulatory challenges posed by such systems. Over 50 countries sent representatives.

In 2002, representatives from well over 50 countries visited FinCEN to discuss new money laundering trends and patterns, details of the USA PATRIOT Act, international case processing, and the regulatory role of FinCEN. Additionally, FinCEN hosted delegations from the Caribbean, the Middle East, Africa, Southeast Asia and the Pacific, Central and South America, the Gulf States, and Europe for more intensive seminars in computer software programs, data mining, and case processing.

Internal Revenue Service (IRS)

In 2002, the IRS Criminal Investigation Division (IRS-CI) increased its commitment to international training, multi-agency training efforts and technical assistance programs to foreign law enforcement agencies.

IRS-CI continues to provide training in Financial Investigative Techniques and Money Laundering at the International Law Enforcement Academies (ILEA) at Bangkok, Budapest and Gaborone. IRS-CI has detailed a special agent to serve as Deputy Director at the ILEA in Bangkok, Thailand. IRS-CI also serves as coordinator of the annual Complex Financial Investigations course provided to senior, mid-level, and first-line law enforcement supervisors, inspectors, investigators, prosecutors and customs officers.

In 2002, IRS-CI also presented training on money laundering, identifying and analyzing financial records, indirect methods of proof, and tracing the proceeds of crime at USG-sponsored seminars for the Royal Thai police, the Philippines, Jamaica, Macedonia, Albania, Hungary, and Bulgaria.

A regional Money Laundering/Financial Investigative Techniques course was also provided in St. Johns, Antigua to various law enforcement officials. The participants represented the nine Caribbean nations, two of which are on FATF's NCCT list. Attending were Anguilla, Antigua, Barbados, Dominica, Grenada, Montserrat, St. Kitts and Nevis, St. Lucia, and St. Vincent and the Grenadines. Similar courses were presented in the Czech Republic and Dar es Salaam, Tanzania.

Country-specific money laundering training was delivered to financial investigators, banking officials, prosecutors, customs agents, revenue agents, bank examiners, judges and police officers in Bogotá, Colombia, Trinidad and Tobago, and Abuja, Nigeria. IRS-CI assisted in conducting a Money Laundering and Evidence Control Training session sponsored by the Department of Justice in Bridgetown, Barbados. Participants included customs and law enforcement officials, prosecutors, and banking regulators.

Office of the Comptroller of the Currency (OCC)

The OCC supported and sponsored several anti-money laundering training initiatives during 2002. Specifically, the OCC: presented four sessions of its four-day Anti-Money Laundering School to foreign banking supervisors in Barbados, Peru, Panama, and Washington, D.C.; presented an anti-money laundering training module in Bank Examination schools for foreign supervisors in Turkey and the United States; and participated in a USAID anti-money laundering training mission to Russia for banking supervisors and industry representatives.

United States Department of Treasury Office of Technical Assistance (OTA)

Treasury's OTA is located within the Office of the Assistant Secretary for International Affairs. The office delivers interactive, advisor-based assistance to senior level representatives in various ministries and central banks in the areas of tax reform, government debt issuance and management, budget policy and management, financial institution reform, and more recently, law enforcement reforms related to money laundering and other financial crimes.

OTA administers the Enforcement Program, a long-term, advisor-based program comprised of a group of approximately 50 experienced advisors with backgrounds in various related areas. Through the use of intermittent and resident advisors the Enforcement Program focuses on the development of legal foundations, policies, and organizations in three areas: (1) money laundering, terrorist financing and other financial crimes, (2) organized crime and corruption, and (3) the reorganization of law enforcement and financial entities in developing economies to help them prevent, detect, investigate and prosecute complex international financial crime.

In 2002, advisors provided assistance to the governments of Albania, Armenia, Azerbaijan, Bosnia, Bulgaria, El Salvador, Guatemala, Hungary, Macedonia, Moldova, Montenegro, Nigeria, Paraguay, Romania, Russia, South Africa, Tanzania, Thailand, Uganda, Ukraine, Honduras, Poland, Serbia and the Eastern Caribbean countries.

OTA conducted several assessments of anti-money laundering regimes in 2002, often working in concert with the U.S. Embassy and/or international bodies. These assessments addressed legislative, regulatory, law enforcement and judicial components of the various programs. The assessments included the development of technical assistance plans to enhance a country's efforts to fight money laundering and terrorist financing. In 2002, such assessments were carried out in Georgia, Montenegro, Peru, Senegal, Ethiopia, Uganda, Tanzania, Ghana, Guinea, Nicaragua, Bangladesh and Burkina Faso.

In 2002, OTA sponsored money-laundering seminars in Azerbaijan, El Salvador, Moldova and Paraguay. The seminars were attended by government officials, bankers and businesspeople, and addressed effective anti-money laundering regimes, terrorist financing, bank examination procedures, financial analysis units and methodologies of detecting and reporting suspicious financial transactions.

United States Customs Service/Operation Green Quest

The U.S. Customs Service (Customs) and its Operation Green Quest are extensively involved in multi-agency international money laundering and financial-related terrorism training programs. The Financial Terrorist Investigations Training seminar is an introduction to international money laundering linked to terrorism. This course is specifically designed to address terrorism, its relationship to money laundering, and country-specific problems. Charities and alternative remittance systems are also covered, and specifically, their use by terrorists. This training was conducted for officials from various nations, including Armenia, Australia, Azerbaijan, Barbados, China, Cyprus, Dominican Republic, Egypt, Georgia, Guyana, Hungary, Jordan, Kazakhstan, Kyrgyzstan, Morocco, Pakistan, Philippines, Russia, St. Kitts and Nevis, Suriname, Tajikistan, Thailand, Trinidad, Turkey, United Arab Emirates and Uzbekistan.

Customs also provides training that covers the use of free trade zones, offshore banking practices, international monetary flows, bulk-cash and electronic funds transfers, and capital flight. Specialized sessions address the black market peso exchange system, the Money Laundering Coordination Center, and/or an overview of Operation Green Quest.

United States Secret Service

The Secret Service continues to send instructors to the International Law Enforcement Academies (ILEA) in Budapest, Hungary, Bangkok, Thailand and Gaborone, Botswana; providing training and strategies to foreign police representatives in the detection of counterfeit U.S. currency and fraud schemes. The Secret Service's established relationship with the counterfeit suppression program also has generated training at the ILEA sites.

Bilateral overseas development includes training and education for law enforcement, prosecutors and financial officials. An integral part of the Secret Service's efforts in this area is the Combating Economic Fraud and Counterfeiting Seminar. In 2002, this seminar was offered to representatives from Trinidad, Bulgaria, Romania, Macedonia, Turkey, Dominican Republic, and Bulgaria.

Department of Justice

During 2002, the Justice Department's Office of Overseas Prosecutorial Development Assistance and Training (OPDAT) and Asset Forfeiture and Money Laundering Section (AFMLS) continued to provide training to foreign prosecutors, judges and law enforcement officials. The seminars provided by OPDAT and AFMLS enhance the ability of participating countries to prevent, detect, investigate, and prosecute money laundering, and to make appropriate and effective use of asset forfeiture. The content of individual seminars varies depending on the specific needs of the participants, but topics addressed in 2002 included developments in money laundering legislation and investigations, the international standards for an anti-money laundering and terrorist financing regime, illustrations of the methods and techniques to effectively investigate and prosecute money laundering, inter-agency cooperation and communication, criminal and civil forfeiture systems, the importance of international cooperation, and the role of prosecutors.

In 2002, in-depth sessions of this seminar were presented to representatives from Antigua, Armenia, Barbados, Bosnia and Herzegovina, Croatia, Dominica, Georgia, Grenada, Hungary, Macedonia, Mexico, Russia, St. Kitts and Nevis, St. Lucia, St. Vincent, Thailand and the United Arab Emirates.

In 2002, OPDAT, with funding from the Department of State's Anti-Terrorism Assistance Program, organized a number of programs aimed at strengthening counter-terrorism laws abroad. Officials from several regions, including Central Asia, the Middle East, the Caucasus and Russia, Southeast Asia, South Asia, Latin America and Africa, participated in seminars focused on counter-terrorism legislation. The seminars addressed trends in international terrorism, international conventions and agreements, basic investigative tools needed to combat terrorism (e.g., electronic surveillance, wiretaps, undercover operations), methods of financing terrorism, extradition and mutual legal assistance, border security and immigration, export controls, weapons of mass destruction, and model legislation. AFMLS and other US agencies provided instructors for each of the courses. Country groups worked with US experts during the seminar to develop action plans to strengthen their countries' counter-terrorism infrastructures. These programs were presented to representatives from Azerbaijan, Armenia, Bangladesh, Chile, Cote d'Ivoire, Cyprus, Djibouti, El Salvador, Egypt, Georgia, Guatemala, Guyana, India, Indonesia, Jordan, Kazakhstan, Kenya, Kyrgyzstan, Laos, Malaysia, Maldives, Morocco, Nepal, Pakistan, Paraguay, Peru, Philippines, Russia, Sierra Leone, South Africa, Sri Lanka, Tajikistan, Thailand, Turkey, United Arab Emirates and Uzbekistan.

With funding from the Department of State and the assistance of attorneys from AFMLS and the Department of Justice's Counter-terrorism Section, OPDAT implemented "The Financial Underpinnings of Terrorism Program," which provides intensive seminars covering all aspects of identifying and prosecuting methods of financing terrorism. An initial session for senior policy officials is followed by a longer, more hands-on session for investigators, judges and prosecutors. Officials from the Philippines and Turkey participated in these programs. A daylong roundtable on this topic was held in Washington, D.C., in September 2002 for a Saudi Arabian delegation, and a regional seminar for officials from Brazil, Panama, Paraguay, Argentina and Venezuela took place in December 2002.

With funding from the Department of State, OPDAT has organized several conferences at International Law Enforcement Academies (ILEA) relating to terrorism. In Bangkok, in March 2002, OPDAT and the International Criminal Investigative Training Assistance Program (ICITAP) organized a conference to address regional concerns involving terrorism. More than 30 senior criminal justice officials from Brunei, Cambodia, Hong Kong, Indonesia, Laos, Macao, Malaysia, China, Philippines, Singapore, Thailand and Vietnam exchanged views and experiences on tactics used by terrorist groups, anti-terrorism financing measures, and the prospects for regional anti-terrorism cooperation. AFMLS and the Counter-terrorism Section supplied instructors.

In March 2002, OPDAT organized a regional conference at the ILEA in Budapest on the subject of money laundering, and AFMLS provided instructors. Issues addressed included international standards for legislation and investigations, the role of the FATF, asset forfeiture, mutual legal assistance and legislation countering money laundering, particularly as it relates to terrorist financing. Thirty-eight senior government officials from Azerbaijan, Georgia, Kazakhstan, Moldova, Russia and Ukraine attended.

In June 2002, OPDAT organized a second conference at the ILEA in Budapest to address regional approaches to investigating and prosecuting organized crime, with a large portion of the discussion focusing on money laundering and asset forfeiture, focusing on terrorist financing and international cooperation. Fifty prosecutors from Azerbaijan, Georgia, Kazakhstan, Moldova, Russia, Ukraine and Uzbekistan attended.

25. Please identify areas, if any, of any incomplete implementation of the Taliban/Al Qaida sanctions regime, and where you believe specific assistance or capacity building would improve your ability to implement the above sanctions regime.

26. Please include any additional information you believe pertinent.

United Nations S/AC.37/2003/(1455)/27

Security Council

Distr.: General
22 April 2003

Original: English

Security Council Committee established pursuant to resolution 1267 (1999)

Note verbale dated 17 April 2003 from the Permanent Mission of Austria to the United Nations addressed to the Chairman of the Committee

The Permanent Mission of Austria to the United Nations presents its compliments to the Chairman of the Security Council Committee established pursuant to resolution 1267 (1999) and has the honour to convey the information requested in paragraph 6 of Security Council resolution 1455 (2003) of 17 January 2003.

03-35101 (E) 040603

Annex to the note verbale dated 17 April 2003 from the Permanent Mission of Austria to the United Nations addressed to the Chairman of the Committee

Report of Austria to the Security Council Committee established pursuant to resolution 1267 (1999) in accordance with paragraph 6 of Security Council resolution 1455 (2003) of 17 January 2003

United Nations Security Council Resolution 1455 (2003) calls upon all States to report to the Security Council Committee established pursuant to resolution 1267 (1999) hereinafter referred to as "the Committee" within 90 days from the date of adoption of this resolution on the steps they have taken to implement the measures required by paragraph 4 (b) of resolution 1267 (1999), paragraph 8 (c) of resolution 1333 (2000) and paragraphs 1 and 2 of resolution 1390 (2002).

The present report is set out according to the guidelines prepared by the Committee on 4 March 2003 and includes answers to those questions where information is available or its submission would not compromise investigations or enforcement actions. Information already provided, however, have not been repeated.

Description of activities by Usama Bin Laden, Al-Qaida, the Taliban and their associates in Austria, the threat they pose to the country and the region, as well as likely trends

There is no evidence of activities by Usama Bin Laden, Al-Qiada, the Taliban and their associates in Austria nor does there exist an immediate threat. Only one still pending criminal proceeding raised suspicion about a possible connection to Al-Qaida.

How is the 1267 Committee's List incorporated within the Austrian legal system and administrative structure

A comprehensive answer has been given in Austria's first report to the Committee. In addition and as regards the prevention of entry into or the transit through Austria, all persons listed are included in a national list. Beside the Schengen Information System (SIS) all persons of whom the necessary data (first and family name as well as date and place of birth) are known have been included in the national EKIS-system (electronic information system on criminal investigation). Information about persons where basic data are not available (in particular the date and place of birth) are kept with the competent authorities, Staatsschutzbehörden (state security authorities).

Problems with the implementation with regard to the names and identifying information as currently included in the List

In those cases where only incomplete data are available (in particular not all relevant first and family names and not the date and place of birth) it is technically difficult to clearly identify the person.

National legislation to prevent entities and individuals from recruiting or supporting Al-Qaida members in carrying out activities inside Austria, and to prevent individuals from participating in Al-Qaida training camps established in Austria or in another country

In its third report to the Counter-Terrorism Committee (CTC) established under Article 6 of United Nations Security Council Resolution 1373 (2001), Austria submitted the following under point 1.7.:

Section 278b of the Austrian Penal Code criminalizes the leading of and the participation in a terrorist group. For the purpose of further defining the meaning of "participation" Section 278b para. 3 refers to Section 278 para. 3 of the Penal Code which stipulates that anybody who inter alia supports a (criminal) group by providing information or assets or in any other way with the awareness that he/she thereby promotes the group or its criminal acts participates as member in the group. As has been pointed out explicitly in the explanatory memorandum to the government bill that introduced this concept, "recruiting" is an example for such a support "in another way".

Financial and Economic Assets Freeze

In Austria's first report to the Committee the legal basis, i.e. EC Council Regulation No 881/2002 of 27 May 2002, has been annexed. This regulation has been amended fifteen times and obliges in article 5 natural and legal persons, entities and bodies to cooperate and to provide relevant information about all funds and economic resources belonging to, or owned or held by, a natural or legal person, group or entity designated by the Committee.

In addition to the provisions in the EC regulation, the Oesterreichische Nationalbank stays in regular contact with all banks as well as other financial institutions in Austria and requires them to report whether or not funds have been frozen. Up to now only one account with an approximate amount of 4.000 US $ has been frozen.

Travel Ban

As stated above all names have been included in either the Schengen Information System (SIS), the national EKIS-system or are kept with the competent authorities, the Staatsschutzbehörden, depending on the level of detail of the data available. All border checkpoints as well as consular offices have access to the national EKIS-system which is updated on a day-to-day basis. Up to now, however, no one of the listed individuals has been stopped.

Arms Embargo

A comprehensive answer to this issue has been given in Austria's first report to the Committee.